Finite Fields and Their Applications 15 (2009) 569–579

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Halving for the 2-Sylow subgroup of genus 2 curves over binary fields

J.M. Miret [a,1], R. Moreno [a,1], J. Pujolàs [a,*,1], A. Rio [b,2]

[a] Dept. de Matemàtica, Universitat de Lleida, Jaume II 69, 25001 Lleida, Spain
[b] Dept. de Matemàtica Aplicada II, Universitat Politècnica de Catalunya, Jordi Girona 1–3, Barcelona, Spain

ARTICLE INFO

Article history:
Received 12 December 2007
Available online 16 June 2009
Communicated by James W. P. Hirschfeld

Keywords:
Genus 2 curves
Jacobian
Binary fields
2-Sylow subgroup

ABSTRACT

We give a deterministic polynomial time algorithm to find the structure of the 2-Sylow subgroup of the Jacobian of a genus 2 curve over a finite field of characteristic 2. Our procedure starts with the points of order 2 and then performs a chain of successive halvings while such an operation makes sense. The stopping condition is triggered when certain polynomials fail to have roots in the base field, as previously shown by I. Kitamura, M. Katagi and T. Takagi. The structure of our algorithm is similar to the already known case of genus 1 and odd characteristic.

1. Introduction

Our interest is in the group of $\mathbb{F}_{2^m}$-points of the Jacobian variety Jac(C) of a genus 2 curve C over $\mathbb{F}_{2^m}$. As is well known, this is isomorphic to the group of $\mathrm{Gal}(\overline{\mathbb{F}}_{2^m}\setminus\mathbb{F}_{2^m})$-invariant elements of $\mathrm{Pic}^0(C)$, the degree zero divisor classes modulo principals on C.

The computation of the order of such groups is generally hard and expensive. However, the order and also the structure of certain subgroups may be easier to find. The object of this paper is the determination of the structure of the subgroup of degree zero divisor classes of order any power of 2, namely the 2-Sylow subgroup of $\mathrm{Jac}(C)(\mathbb{F}_{2^m})$ – which we write $\mathrm{Jac}[2^\infty]$ from now on. We provide a deterministic polynomial time algorithm to do so. Since our method is built on purpose to find

* Corresponding author.
E-mail addresses: miret@matematica.udl.cat (J.M. Miret), ramiro@matematica.udl.cat (R. Moreno), jpujolas@matematica.udl.cat (J. Pujolàs), ana.rio@upc.edu (A. Rio).

[1] Partial support from MTM2007-66842-C02-02.
[2] Partial support from MTM2006-15038-C02-01 and 2005SGR 00443.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2009.05.007

Jac[2^∞], it is more efficient than the algorithms for the whole group of $\mathbb{F}_{2^m}$-rational points. The knowledge of Jac[2^∞] at a cheaper price may have some interesting advantages.

As for the genus 1 case, an algorithm for the determination of ℓ-Sylow subgroups of elliptic curves over $\mathbb{F}_p$ with $\ell \neq p$ and $p \neq 2$ was given in [15]. The approach in [15] relied on iterated solutions to the equation $[2]P = W$, starting with the points W of order 2. Such a *halving* procedure (this is the usual name for the reverse operation of the natural multiplication by 2 map) received some attention in the crypto community for elliptic curves over binary fields (see [12,16]). However, we are not aware of the use of halving to determine the 2-Sylow subgroups neither for elliptic curves nor Jacobians of genus 2 curves in characteristic 2.

Our method is a genus 2 adaptation of the $\ell \neq 2$ elliptic curve case using an iteration of the halving operation in Jac(C)($\mathbb{F}_{2^m}$). A halving algorithm for genus 2 curves over binary finite fields was given in [11]. It is an interesting problem to use the analogues of the ℓ-division polynomials for Jacobians of curves of genus 2 to obtain a genus 2 version of [15] in any characteristic.

2. Degree zero divisor classes of order 2

We recall some basics about the group Jac(C)($\mathbb{F}_{2^m}$) for C a non-singular curve of genus 2 over $\mathbb{F}_{2^m}$. We assume that C has at least one Weierstraß point P_∞ with coordinates in our base field $\mathbb{F}_{2^m}$. Under this assumption C has a Koblitz model

$$\mathrm{C} : y^2 + h(x)y = f(x)$$

with $f(x) = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{F}_{2^m}[x]$ and $h(x) = h_2x^2 + h_1x + h_0 \in \mathbb{F}_{2^m}[x]$ nonzero.

For every value of x, the two roots of the quadratic polynomial in y above give the two points of C conjugated by the hyperelliptic involution $\iota : (x, y) \to (x, y + h(x))$. The double solutions are the Weierstraß points of C (note that P_∞ is another such point), and since $y \to y^2$ is bijective for fields of even characteristic, the x coordinate of the Weierstraß points (other than P_∞) is given by the roots of $h(x)$.

Due to the Rieman–Roch Theorem, the nontrivial elements $D \neq (1, 0)$ of the group Jac(C)($\mathbb{F}_{2^m}$) take two forms according to the number of points in the finite part of D. The *weight one* divisors are $P_1 - P_\infty$ with $P_1 = (x_1, y_1) \in \mathrm{C}(\mathbb{F}_{2^m})$. The *weight two* divisors are $D = P_1 + P_2 - 2P_\infty$ where $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ are (possibly equal) points of C whose coordinates satisfy the condition that there is a pair of polynomials $u(x), v(x) \in \mathbb{F}_{2^m}[x]$ such that

$$u(x) = (x + x_1)(x + x_2), \qquad v(x_1) = y_1, \qquad v(x_2) = y_2, \qquad \deg\big(v(x)\big) < 2,$$
$$v(x)^2 + h(x)v(x) + f(x) \equiv 0 \pmod{u(x)}.$$

Note that $v(x)$ is the unique polynomial of degree $\leqslant 1$ in $\mathbb{F}_{2^m}[x]$ that interpolates the points P_1, P_2. Note also that the coefficients of $u(x)$ and $v(x)$ are in $\mathbb{F}_{2^m}$ while x_1, x_2, y_1, y_2 don't need to for a general weight two divisor. We write such a $D \in \mathrm{Jac(C)}(\mathbb{F}_{2^m})$ as $D = (u(x), v(x))$ in what follows. One refers to $u(x)$ and $v(x)$ as the *first* and *second* coordinate of D respectively. Weight one divisors we write as $D = (x + x_1, y_1)$.

In Jac(C) the pairs that differ by divisors of functions on C are identified. For instance $P_1 = (x_1, y_1)$ and $P_1^\iota = (x_1, y_1 + h(x_1))$ constitute the divisor of zeros of the function $x(P) - x_1$. Such a divisor is sometimes called *hyperelliptic*. Analogously, every hyperelliptic divisor is associated to a function, and they all become zero in the divisor class group. Since any Weierstraß point W of C is conjugate to itself, $2W$ is a hyperelliptic divisor. It follows that the weight one divisors with a Weierstraß point in the finite support have order 2, and of course this is true also for sums of such divisors. Hence the weight two divisors with Weierstraß points in the finite support are order 2 as well. We write Jac[2] for the subgroup of divisors of order 2 and Jac[2^∞] for the 2-Sylow subgroup of Jac(C), i.e. the subgroup of divisors of order any power of 2. Since our base field has even characteristic, it is well known that Jac[2] is either trivial, or isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or otherwise isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Because multiplication by any integer is an inner operation for cyclic subgroups, it follows that Jac[2^∞] has the same rank as Jac[2]. Since the Weierstraß points have order 2, it is a matter of showing enough independent Weierstraß points to obtain the rank of Jac[2^∞].

If $h(x) = h_1 x + h_0$ with $h_1 \neq 0$ then Jac[2] is generated by the weight one divisor

$$W = \left(x + \frac{h_0}{h_1}, \sqrt{f\left(\frac{h_0}{h_1}\right)}\right)$$

and Jac[2^∞] is rank 1. If $h_1 = 0$ and $h_0 \neq 0$ then Jac[2] is trivial because the discriminant of the curve equation never vanishes.

The rank 2 case happens if $h(x) = h_2 x^2 + h_1 x + h_0$, with $h_2 \neq 0$, splits into linear factors $h(x) = h_2(x+\alpha)(x+\beta)$ with $\alpha, \beta \in \mathbb{F}_{2^m}$. The 2-torsion subgroup Jac[2] $\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is generated in this case by any pair among the weight one divisors

$$W_1 = \left(x + \alpha, \sqrt{f(\alpha)}\right), \qquad W_2 = \left(x + \beta, \sqrt{f(\beta)}\right)$$

and their weight two sum

$$W_1 + W_2 = \left(\frac{h(x)}{h_2}, \sqrt{f(\beta)}\left(\frac{x+\alpha}{\alpha+\beta}\right) + \sqrt{f(\alpha)}\left(\frac{x+\beta}{\alpha+\beta}\right)\right). \tag{1}$$

The second coordinate above is the standard Lagrange interpolation polynomial and obviously lies in $\mathbb{F}_{2^m}[x]$ as long as α and β belong to $\mathbb{F}_{2^m}$. If $h(x)$ is degree 2 with no roots in $\mathbb{F}_{2^m}$ there is only one Weierstraß divisor W defined over $\mathbb{F}_{2^m}$, and it is given by the same expression (1). Note that the second coordinate is fixed under permutation of the roots $\alpha, \beta \in \mathbb{F}_{2^{2m}}$, hence it is also defined over $\mathbb{F}_{2^m}$. This implies that the rank of Jac[2] is 1 over the base field – and clearly 2 over a quadratic extension. Finally, if $h(x)$ is degree 2 with a double root $\alpha \in \mathbb{F}_{2^m}$, the rank of Jac[2] is also 1, the generator being

$$W_1 = \left(x + \alpha, \sqrt{f(\alpha)}\right)$$

if $f'(\alpha) \neq 0$ and

$$W_1 = \left((x+\alpha)^2, \sqrt{f(\alpha)}\right)$$

if $f'(\alpha) = 0$. We just proved the following.

Lemma 2.1. *Let $C/\mathbb{F}_{2^m}$ be a genus 2 curve over $\mathbb{F}_{2^m}$ given in Koblitz form. Then the group* Jac[2^∞] *has rank 2 if $h(x)$ is quadratic split with two distinct roots in $\mathbb{F}_{2^m}$. If* $\deg(h(x)) = 1$ *or $h(x)$ is quadratic irreducible or $h(x)$ is quadratic with a double root in $\mathbb{F}_{2^m}$, then* Jac[2^∞] *has rank* 1. *If $h(x)$ is constant then* Jac[2^∞] *is trivial.*

From now on we assume $\deg(h(x)) = 1$ or 2. Our procedure outputs generators for Jac[2^∞] and their orders, and the first step to do so consists in building up the above generators of Jac[2] as seeds for the halving iteration described in the next section.

Algorithm. (SeedBuildUp)

INPUT: the base field $\mathbb{F}_{2^m}$ and the polynomials $f(x), h(x) \in \mathbb{F}_{2^m}[x]$ of C.
OUTPUT: a set W of generators of Jac[2]

1. if $\deg(h(x)) = 1$ then $\alpha \leftarrow \text{Roots}(h(x))[1]$, $y_\alpha \leftarrow \sqrt{f(\alpha)}$, $W \leftarrow (x+\alpha, y_\alpha)$
2. if $\deg(h(x)) = 2$ and $h(x)$ is irreducible then

3. extend base field $\mathbb{F}_{2^m}$ by $h(x), \alpha \leftarrow$Roots$(h(x))[1]$, $\beta \leftarrow$Roots$(h(x))[2]$,
   $y_\alpha \leftarrow \sqrt{f(\alpha)}$, $y_\beta \leftarrow \sqrt{f(\beta)}$, $y_{LI} \leftarrow y_\beta(\frac{x+\alpha}{\alpha+\beta}) + y_\alpha(\frac{x+\beta}{\alpha+\beta})$, $W \leftarrow (\frac{h(x)}{h_2}, y_{LI})$
4. if $\deg(h(x)) = 2$ and $h(x)$ has a root in $\mathbb{F}_{2^m}$ then
5. if $h_1 = 0$ then $\alpha \leftarrow$Roots$(h(x))[1]$, $df \leftarrow f'(\alpha)$
6. if $df \neq 0$ then $y_\alpha \leftarrow \sqrt{f(\alpha)}$, $W \leftarrow (x+\alpha, y_\alpha)$
7. else $y_\alpha \leftarrow \sqrt{f(\alpha)}$, $W \leftarrow ((x+\alpha)^2, y_\alpha)$
8. if $h_1 \neq 0$ then $\alpha \leftarrow$Roots$(h(x))[1]$, $\beta \leftarrow$Roots$(h(x))[2]$, $y_\alpha \leftarrow \sqrt{f(\alpha)}$,
   $y_\beta \leftarrow \sqrt{f(\beta)}$, $W_1 \leftarrow (x+\alpha, y_\alpha)$, $W_2 \leftarrow (x+\beta, y_\beta)$, $W_3 \leftarrow W_1 + W_2$,
   $W \leftarrow$ choose two among $\{W_1, W_2, W_3\}$

In a broader context, the first step to provide divisor classes of 2-power order in Jacobians of hyperelliptic curves of genus larger than 2 relies also in the computation of enough Weierstraß points of C. There are well-known algorithms to compute such points for quite general curves (see [9,10]), and one might try to use them as seeds to work out the corresponding Sylow subgroups of their Jacobians.

3. Halving loop

A key step in our algorithm is to reverse the group law in Jac(C)$(\mathbb{F}_{2^m})$, which constructs first the formal sum of divisors, called the *composition*, and then chooses the *reduced* representative. The second step involves detection of principal divisors in the support and erasing them off. In practice these two manipulations are executed in terms of coordinates $(u(x), v(x))$ by Cantor's algorithms [4]. In the particular case of adding a divisor class with itself, the composition and reduction steps form the following algorithm.

Algorithm. (DOUBLING)

INPUT: $D_1 = (U_1(x), V_1(x))$
OUTPUT: $D_2 = (U_2(x), V_2(x)) = 2D_1$

1. $U_1'(x) \leftarrow U_1^2(x)$
2. $S(x) \leftarrow (f(x) + h(x)V_1(x) + V_1^2(x))/U_1(x)$, $S(x) \leftarrow S(x)h^{-1}(x) \bmod U_1(x)$
3. $V_1'(x) \leftarrow S(x)U_1(x) + V_1(x)$
4. $U_2'(x) \leftarrow (f(x) + h(x)V_1'(x) + V_1'^2(x))/U_1'(x)$
5. $U_2(x) \leftarrow Monic(U_2'(x))$
6. $V_2(x) \leftarrow V_1'(x) + h(x) \bmod U_2(x)$

There exist variants of DOUBLING which are faster for certain types of curves (see [14]). Reversing the algorithms for doubling it is possible to design *halving* procedures in coordinates (see [2,11]). Birkner's algorithm [2] is faster due to the optimized arithmetic developed in [13,14], even though it does not cover the whole types of curves we are interested in.

The halving algorithm by Kitamura, Katagi and Takagi [11] is based on a search for a polynomial $k(x) = k_1 x + k_0 \in \mathbb{F}_{2^m}[x]$ such that $V_1'(x) + h(x) = V_2(x) + k(x)U_2(x)$ in step 6 of DOUBLING. If such a polynomial exists, then it allows to write $U_1(x), V_1(x)$ in terms of the coefficients of $U_2(x), V_2(x)$ and the polynomials $h(x)$, $f(x)$ from the Koblitz model of C. The existence of $k(x)$ provides a method to reverse the doubling operation as follows.

It is shown in [11] that the coefficients k_1, k_0 are derived from two equations $p_1(x) = 0$ and $p_0(x) = 0$. If we write $U_i(x) = x^2 + u_{i1}x + u_{i0}$ and $V_i(x) = v_{i1}x + v_{i0}$, where $i = 1, 2$, then

$$p_1(x) = u_{21}x^2 + h_2 x + 1,$$

k_1 is a root of $p_1(x)$,

$$p_0(x) = u_{21}x^2 + h_1 x + k_1 h_0 + c_1,$$

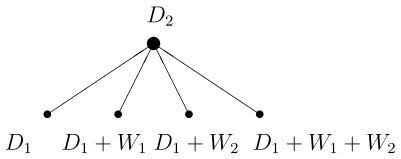

Fig. 1. $\frac{1}{2}D_2$ for non-cyclic 2-torsion Jacobians.

with $c_1 = f_3 + h_2 v_{21} + u_{20} + (f_4 + u_{21})u_{21}$, and k_0 is a root of $p_0(x)$. Given a pair k_1, k_0, the coefficients of $U_1(x)$ are

$$u_{11} = \frac{1}{k_1}\sqrt{k_1 h_1 + k_0 h_2 + k_1^2 u_{20} + k_0^2 + f_4 + u_{21}},$$
$$u_{10} = \frac{1}{k_1}\sqrt{k_0 h_0 + k_0^2 u_{20} + c_0}, \tag{2}$$

where $c_0 = f_2 + h_2 v_{20} + h_1 v_{21} + v_{21}^2 + (f_4 + u_{21})u_{20} + c_1 u_{21}$.

Different pairs of roots k_1', k_0' give rise to different divisors D_1 satisfying $2D_1 = D_2$. We write $\frac{1}{2}D_2$ for the set of all such D_1. It is easy to show that the difference between two elements in $\frac{1}{2}D_2$ lies in Jac[2] (see Fig. 1 for non-cyclic 2-torsion case).

Since we know #Jac[2], it follows that $\#\frac{1}{2}D_2$ is 0 or 2 for cyclic 2-torsion and 0 or 4 for non-cyclic 2-torsion. The behaviour of the cardinal of $\frac{1}{2}D_2$ can be described in terms of the roots of $p_1(x)$, $p_0(x)$ by means of the constructive formulas (2) for the first coordinates $U_1(x)$ of the elements $D_1 = (U_1(x), V_1(x)) \in \frac{1}{2}D_2$. The following result shows that the behaviour of the roots of $p_1(x)$, $p_0(x)$ depends on those of $h(x)$.

Proposition 3.1. *Let* C *be a genus* 2 *curve over* $\mathbb{F}_{2^m}$ *given in Koblitz form. Let* $p_1(x)$, $p_0(x)$ *be the halving polynomials above, built iteratively from the generators of* Jac[2] *given in Lemma* 2.1. *Then at every iteration the following holds*:

(i) *if* $\deg(h(x)) = 1$, *then* $p_1(x)$ *has one double root if any, and* $p_0(x)$ *has no double roots.*
(ii) *if* $h(x)$ *is quadratic irreducible, then* $p_1(x)$ *has no double roots, and if it has roots then exactly one of them leads to a* $p_0(x)$ *with roots, which are different.*
(iii) *if* $h(x)$ *has a double root, then* $p_1(x)$ *has no double roots, and if it has roots then both* $p_0(x)$*'s have one double root.*
(iv) *if* $h(x)$ *has two different roots, then* $p_1(x)$ *has no double roots, and if it has roots then either both of the* $p_0(x)$*'s have two different roots or none of them has roots at all.*

Proof. The claims follow from the criterion which says that $ax^2 + bx + c \in \mathbb{F}_{2^m}[x]$ is reducible if and only if $Tr_{\mathbb{F}_{2^m}/\mathbb{F}_2}(ab/c^2) = 0$, see [11].

Regarding the construction of the second coordinate $V_1(x)$ of the divisor $D_1 = (U_1(x), V_1(x))$ from the first coordinate $U_1(x)$, our approach is different to [11]. We consider all possible linear interpolation polynomials of the 2 (possibly repeated) roots $x_i \in \mathbb{F}_{2^{2m}}$ of $U_1(x)$ at the 4 (possibly repeated) roots y_i, $y_i + h(x_i)$ of the quadratic polynomials $y^2 + h(x_i)y + f(x_i)$ for $i = 1, 2$. Among these possibilities we choose $V_1(x)$ to be the one defined over the base field $\mathbb{F}_{2^m}$ and satisfying $2D_1 = D_2$ (note that $V_1(x)$ may well not exist, in which case no halving of D_2 exists and our loop stops). The interpolation step presents some particularities if the number of $\mathbb{F}_{2^m}$-roots of $U_1(x)$ or the polynomials $y^2 + h(x_i)y + f(x_i)$ is 0 or 1, details which we omit.

We call HALVING the procedure that takes $D_2 = (U_2(x), V_2(x))$ and returns $D_1 = (U_1(x), V_1(x))$ if the constructions of $U_1(x)$ and $V_1(x)$ described above are successful, and returns the input D_2 unaltered otherwise.

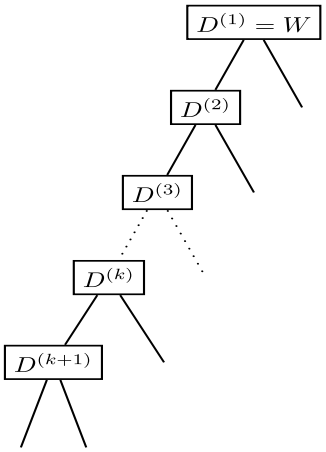

Fig. 2. Binary tree in the case $\mathrm{Jac}[2^\infty] \cong \mathbb{Z}/2^n\mathbb{Z}$.

4. Down the trees

The different types of seeds described in Section 2 produce two different structures for $\mathrm{Jac}[2^\infty]$. Namely, when Jac[2] has 1 or 3 nontrivial elements, the iteration of the HALVING loop in Section 3 forms one binary tree or three quaternary trees respectively. For each of them the nodes at level k are divisors of order 2^k.

For our purpose we are interested only in partial information about these trees. More precisely, in the binary case we have $\mathrm{Jac}[2^\infty] \cong \mathbb{Z}/2^n\mathbb{Z}$ and our aim is twofold: to find the exponent n (which is the height of the tree), and one of the nodes in the bottom (which is a generator of $\mathrm{Jac}[2^\infty]$). In the quaternary case one has $\mathrm{Jac}[2^\infty] \cong \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$, with $1 \leqslant r \leqslant n$, and we want to determine n, r and the corresponding generators of orders 2^n and 2^r. The height of one tree is n and, as we will see, the height of the remaining 2 is the same and equals to r.

4.1. The cyclic cases

We know from Section 2 that Jac[2] is cyclic when $h(x)$ is quadratic irreducible, quadratic with a double root or $\deg(h(x)) = 1$. We describe now the descending procedure down the binary tree (by Proposition 3.1) until the deepest nodes (Fig. 2). We say that a binary tree is *complete* if the nodes with no children are all in the same level.

Lemma 4.1. *Let* C *be a genus* 2 *curve over* $\mathbb{F}_{2^m}$ *given in Koblitz form such that* $\mathrm{Jac}[2] \cong \mathbb{Z}/2\mathbb{Z}$. *Then the binary tree associated to the divisors of order any power of* 2 *is complete.*

Proof. Clearly $\mathrm{Jac}[2^\infty]$ is rank 1 too, and isomorphic to $\mathbb{Z}/2^n\mathbb{Z}$. Let W_{2^∞} be a generator of $\mathrm{Jac}[2^\infty]$. Let $D \in \mathrm{Jac}[2^\infty]$ be a divisor from a different level than W_{2^∞}. This implies $ord(D) = 2^k$ with $0 < k < n$. Since we deal with a cyclic group, the subgroup of order 2^k is generated by $2^{n-k}W_{2^\infty}$. Hence $D = 2(2^{n-k-1}t'W_{2^\infty})$, for some $t' > 0$, and $\frac{1}{2}D$ is nonempty. By Proposition 3.1, $\#\frac{1}{2}D = 2$.

In our algorithm, at each iteration of the halving loop we specify an element D' in $\frac{1}{2}D$ (so a pair k_0, k_1 of roots), starting with the seed $D = \mathcal{W}$. Since the tree is complete, with any choice in $\frac{1}{2}D$ we reach the bottom level. The output of the following algorithm is a generator of $\mathrm{Jac}[2^\infty]$ and its order in the cyclic case.

Algorithm. (2SCyclic)

INPUT: a curve C with $h(x)$ deg one, irred of deg 2 or with a double root.
OUTPUT: the exponent n and a generator W_{2^∞} of Jac$[2^\infty]$

1. $W \leftarrow$SeedBuildUp$(f(x), h(x))$
2. $W' \leftarrow$Halving$(W, f(x), h(x))$
3. $n \leftarrow 1$
4. while $W' \neq W$ do
5. $\quad W \leftarrow W'$
6. $\quad W' \leftarrow$Halving$(W, f(x), h(x))$
7. $\quad n \leftarrow n+1$
8. $W_{2^\infty} \leftarrow W'$

4.2. The rank 2 case

From Section 2, we know that Jac[2] is rank 2 when $h(x)$ is quadratic and splits in $\mathbb{F}_{2^m}$. Hence there are 3 nontrivial elements in Jac[2] producing each of them a quaternary tree. The two exponents n, r in Jac$[2^\infty] \cong \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$ are related to the heights of these trees.

Lemma 4.2. *If $n = r$ then the 3 trees are complete quaternary trees of height n. If $r < n$ then two trees are complete quaternary trees of height r and the remaining tree has height n. Moreover, from level $r+1$ to $n-1$ half of the nodes have no children and the other half have 4 children.*

Proof. If $n = r$ the proof is analogous to that of Lemma 4.1. Assume $r < n$. It is clear that two generators $W^n_{2^\infty}, W^r_{2^\infty}$ of Jac$[2^\infty]$ lie at the bottom of a tree $\mathcal{T}_{W_1}$ of height n hanging from W_1, say, and at the bottom of a tree $\mathcal{T}_{W_2}$ hanging from W_2 respectively. We are going to exhibit now a divisor in the tree $\mathcal{T}_{W_3}$ hanging from $W_3 = W_1 + W_2$ of order 2^r, and the first claim will follow. The divisor $W := 2^{n-r}W^n_{2^\infty} + W^r_{2^\infty}$ satisfies $2^{r-1}W = W_1 + W_2 = W_3$, so it lies in $\mathcal{T}_{W_3}$ and has order 2^r. The proof that up to level r all the trees are complete is analogous to that of Lemma 4.1. We show next that $\mathcal{T}_{W_1}$ is not complete from level $r+1$ onwards. We have #Jac$[2^{r+k}] = 2^{2(r+k)}$ if $-r \leqslant k \leqslant 0$, and #Jac$[2^{r+k}] = 2^{2r+k}$ if $1 \leqslant k \leqslant n-r$. Hence, the number of divisors of order 2^r is $2^{2(r-1)}3$, and the number of divisors of order 2^{r+k} with $1 \leqslant k \leqslant n-r$ is 2^{r+k-1}. Therefore in $\mathcal{T}_{W_1}$ the ratio between the number of divisors of levels $r+1$ and r is 4, which means that all nodes at level r have children. Otherwise the ratio is 2 from level $r+1$ onwards, and by Proposition 3.1 just half the nodes have children.

The descending process down the 3 quaternary trees to reach the bottom line (Fig. 3) is a bit more intricate than in the cyclic cases, and we now explain how we proceed. For our algorithm we need to choose first two seeds W_1, W_2. Next we have to choose an element D'_1 in $\frac{1}{2}D_1$ (starting with $D_1 = W_1$) and also an element D'_2 in $\frac{1}{2}D_2$ (starting with $D_2 = W_2$). As long as $p_0(x)$ and $p_1(x)$ have roots in $\mathbb{F}_{2^m}$, the descending procedure down the trees goes on by choosing any pair k_0, k_1 of roots. Let $r_1 \leqslant r_2$ be the levels down the trees reached from W_1, W_2 respectively by the deepest divisors D_{r_1}, D_{r_2}. Since up to level r the trees are complete, it follows that $r = r_1$ and D_{r_1} becomes a generator $W^r_{2^\infty}$. By definition of n, we have $r_2 = r + k$ for some $k \geqslant 0$.

In order to find n we proceed as follows. Assume first $r_1 < r_2$. This means $k > 1$. Since beyond level $r+1$ some nodes are childless, n could be strictly larger than $r+k$. The following proposition gives a necessary condition for the latter to happen (see [15] for the similar genus 1 case).

Proposition 4.3. *Let D_{r+k} and $W^r_{2^\infty} + D_{r+k}$ as above with $k \geqslant 1$. If* Jac(C)$(\mathbb{F}_{2^m})$ *has a divisor of order 2^{r+k+1}, then either $\frac{1}{2}D_{r+k} \neq \emptyset$ or $\frac{1}{2}(W^r_{2^\infty} + D_{r+k}) \neq \emptyset$.*

Proof. We prove the equivalent statement that $\frac{1}{2}D_{r+k} = \emptyset$ and $\frac{1}{2}(W^r_{2^\infty} + D_{r+k}) = \emptyset$ imply $n = r + k$. Indeed, since Jac$[2^{r+k}] = \langle D_{r+k}, W^r_{2^\infty}\rangle$, for any divisor D' of order 2^{r+k}, the equality $D' = \alpha D_{r+k} +$

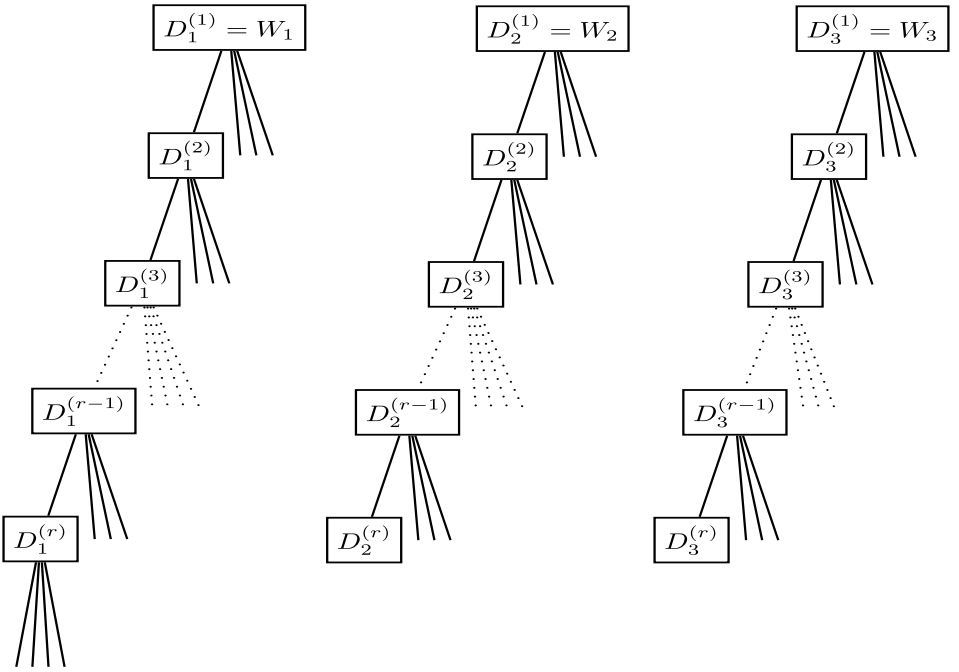

Fig. 3. Trees in the case $\mathrm{Jac}[2^\infty] \cong \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$.

$\beta W_{2^\infty}^r$ must hold. Moreover, since $ord(D') = 2^{r+k}$ one can write $D' = D_{r+k} + \alpha' D_{r+k} + \beta W_{2^\infty}^r$ with α' even and $\beta \geqslant 0$. Then, depending on the parity of β, D' is of the form $D' = D_{r+k} + \alpha' D_{r+k} + \beta W_{2^\infty}^r$ or of the form $D' = D_{r+k} + W_{2^\infty}^r + \alpha' D_{r+k} + \beta' W_{2^\infty}^r$ with α' and β' even. Hence if $\frac{1}{2}D_{r+k}$ and $\frac{1}{2}(D_{r+k} + W_{2^\infty}^r)$ are empty then $\frac{1}{2}D' = \emptyset$ for all D' of order 2^{r+k} and $n = r + k$.

By Proposition 4.3 above, to obtain n we shall keep adding $W_{2^\infty}^r$ every time a childless node is hit. If adding $W_{2^\infty}^r$ provides a childless node again, the deepest level n is reached.

Assume now $r_1 = r_2$ (so $k = 0$ and $r = r_1$). The divisor $D_{r_1} + D_{r_2}$ belongs to the tree $\mathcal{T}_{W_3}$. Hence this third tree is at least as high as $\mathcal{T}_{W_1}$ and $\mathcal{T}_{W_2}$, but could still be higher. If $D_{r_1} + D_{r_2}$ is childless then $n = r$. Otherwise the same procedure as in the case $r_1 < r_2$ applies. The following algorithm summarizes the above steps to find n, r.

Algorithm. (2SRANK2)

INPUT: a curve C with $h(x)$ of degree 2 and two different roots in $\mathbb{F}_{2^m}$ OUTPUT: the exponents n, r and generators $W_{2^\infty}^n, W_{2^\infty}^r$ of $\mathrm{Jac}[2^\infty]$

1. $W_1, W_2 \leftarrow$SEEDBUILDUP$(f(x), h(x))$
2. for $i = 1, 2$ do
3. $\quad n_i \leftarrow 1$
4. $\quad W_i' \leftarrow$HALVING$(W_i, f(x), h(x))$
5. $\quad$ while $W_i' \neq W_i$ do
6. $\quad\quad W_i \leftarrow W_i'$, $n_i \leftarrow n_i + 1$
7. $\quad\quad W_i' \leftarrow$HALVING$(W_i, f(x), h(x))$
8. if $n_1 = n_2$then
9. $\quad W_3 \leftarrow W_1 + W_2$, repeat 4. to 7. with $i \leftarrow 3$, $n_3 \leftarrow n_1$

10. if $n_3 = n_1$ then $[n, r] \leftarrow [n_1, n_1]$, $W^n_{2^\infty} \leftarrow W_1$, $W^r_{2^\infty} \leftarrow W_2$
11. else $n_2 \leftarrow n_3$, $W_2 \leftarrow W_3$
12. if $n_1 \neq n_2$ then $n_{min} \leftarrow Min(n_1, n_2)$, $n_{max} \leftarrow Max(n_1, n_2)$
13. if $n_{min} = n_1$ then $W_{min} \leftarrow W_1$, $W_{max} \leftarrow W_2$
14. if $n_{min} = n_2$ then $W_{min} \leftarrow W_2$, $W_{max} \leftarrow W_1$
15. $W_{max} \leftarrow W_{max} + W_{min}$, $W'_{max} \leftarrow$HALVING$(W_{max}, f(x), h(x))$
16. while $W'_{max} \neq W_{max}$ do
17. $n_{max} \leftarrow n_{max} + 1$
18. repeat 4. to 7. with $W_i \leftarrow W'_{max}$
19. $W_{max} \leftarrow W_{max} + W_{min}$
20. $[n, r] \leftarrow [n_{max}, n_{min}]$, $W^n_{2^\infty} \leftarrow W_{max}$, $W^r_{2^\infty} \leftarrow W_{min}$

5. Some examples

The algorithms SEEDBUILDUP, HALVING, 2SCYCLIC and 2SRANK2 from the previous sections have been coded in Magma [3]. We generated[3] random curves over $\mathbb{F}_{2^m}$ with $m = 160$. It took a considerably large amount of time to find examples of curves with a large 2-Sylow subgroup, but even in these cases our method returns the structure and generators of $\mathrm{Jac}[2^\infty]$ in a matter of seconds.

The number of iterations that our algorithm takes to find n, r is bounded by the 2-adic valuation $v_2(|\mathrm{Jac}(C)(\mathbb{F}_{2^m})|) \leqslant 2m$. The complexity of every iteration is essentially equivalent to the extraction of a root of a quadratic polynomial in $\mathbb{F}_{2^m}[x]$, whose cost is $O(m^3)$ [1]. The overall computational effort is thus $O(m^4)$.

For the curve

$$y^2 + \left(x^2 + x\right)y = x^5 + x^3 + x^2 + x$$

we found

$$\mathrm{Jac(C)}(\mathbb{F}_{2^{160}})\left[2^\infty\right] = \mathbb{Z}/2^6\mathbb{Z} \times \mathbb{Z}/2^6\mathbb{Z}$$

and

$$\mathrm{Jac(C)}(\mathbb{F}_{2^{1024}})\left[2^\infty\right] = \mathbb{Z}/2^{11}\mathbb{Z} \times \mathbb{Z}/2^{11}\mathbb{Z}.$$

We show some other examples of our findings in Table 1, where the coefficients of the curve are coded in hexadecimal notation.

We used our algorithm further to study the distribution of curves C over $\mathbb{F}_4$ and $\mathbb{F}_8$ with respect to the structure of their 2-Sylow subgroups. The result of our search is shown in Tables 2 and 3. The amount of curves for each pair (n, r) is given in the third column, and the fourth shows the number of curves identifyed modulo isomorphisms preserving infinity (see [7,8]). The resulting classes are distributed in reverse order with respect to $\deg(h(x))$ ([7,8], Types I, II, III) in the last three columns. Notice the missing $(3, 2)$ in Table 2 and $(3, 2)$, $(4, 2)$ in Table 3.

Isomorphisms moving infinity were taken into account in [5], where the classification into isomorphism classes was done via the ramification divisor of the hyperelliptic morphism from C to $\mathbb{P}^1$. Following the notation in [5], the representatives modulo isomorphism (now considering the isomorphisms moving ∞ as well) fall into five cases, named $(1, 1, 1)$-split, $(1, 1, 1)$-quadratic, $(1, 1, 1)$-cubic, $(1, 3)$ and (5) after the coefficients of the *different exponent*. Using such a classification, the case $(1, 3)$ includes all curves with $h(x)$ linear (those of Type II following the classification above) and $h(x)$ with a double root (included in Type I above). The remaining Type I curves fall into the cases $(1, 1, 1)$-split (in case $h(x)$ has two different roots in the base field) and $(1, 1, 1)$-quadratic (in case $h(x)$ is

[3] We would like to thank Javier Valera for his help throughout this section.

Table 1
Examples over $\mathbb{F}_{2^{160}}$.

$m = 160$	
f_0	E68FA52E53F329B854A56E5DD25BC3CE4366D961
f_1	E63C51B3F0597362D57C60D0587AB34946C2C52F
f_2	F793C9A2FBF0ACA126A2601296A0795C4407B021
f_3	DC9698460E8D844A262078404A93DBFF909C42BD
f_4	1890AC026BE960F9D335CC9D5A9659966D4570D3
h_0	868940E616F083DC305949C036E2EE7F80368C3C
h_1	02B2C18C4244144E14BB7BE2841DCAADF9F15C7E
h_2	1
(n, r)	(19,0)
f_0	7B1F6111127A6ACD4E8E9AC0B09BF149A899DA6D
f_1	2CADF5D366C41204AEF45DC831793DF62764119C
f_2	3BBF9610411DBDC0DF69668F513684BCD8612990
f_3	76958D6692E4DA8C4CEF3C2E9FF8AAF4B18CA207
f_4	A8B6D32F2BFF8CBEAC063F9B87F35DC314868AA1
h_0	3DADAD6D0F99106AEC3625E0A4A2B9A34601EBDA
h_1	7C56DA1EE08BA433EFA629D222DD151CDCA6DF95
h_2	1
(n, r)	(13,2)

Table 2
Distribution of (n, r) for all Koblitz curves over $\mathbb{F}_4$.

$n + r$	(n, r)	# curves	# classes	I	II	III
0	(0,0)	3072	14	0	0	14
1	(1,0)	20736	54	42	12	0
2	(2,0)	7680	20	14	6	0
	(1,1)	5568	16	16	0	0
3	(3,0)	5376	16	11	5	0
	(2,1)	1152	3	3	0	0
4	(4,0)	1152	4	3	1	0
	(3,1)	2304	6	6	0	0
	(2,2)	192	1	1	0	0
5	(5,0)	768	2	2	0	0
	(4,1)	1152	4	4	0	0

Table 3
Distribution of (n, r) for all Koblitz curves over $\mathbb{F}_8$.

$n + r$	(n, r)	# curves	# classes	I	II	III
0	(0,0)	229376	30	0	0	30
1	(1,0)	5218304	364	308	56	0
2	(2,0)	2179072	152	124	28	0
	(1,1)	2143232	160	160	0	0
3	(3,0)	1060864	86	73	13	0
	(2,1)	1290240	90	90	0	0
4	(4,0)	473088	42	39	3	0
	(3,1)	567296	42	42	0	0
	(2,2)	129024	12	12	0	0
5	(5,0)	344064	24	18	6	0
	(4,1)	325606	24	24	0	0
6	(6,0)	258048	18	12	6	0
	(5,1)	397338	30	30	0	0
	(3,3)	64512	6	6	0	0

Table 4
Number of classes preserving infinity for Type I curves.

$h(x)$ irreducible in $\mathbb{F}_q$	$(q-1)(q^2+\frac{1}{2}q-2)$
$h(x)$ with 2 different roots in $\mathbb{F}_q$	$q(q-1)(q-\frac{3}{2})$
$h(x)$ with a double root in $\mathbb{F}_q$	$2q(q-1)$

degree 2 irreducible). Type III curves (where $h(x)$ is a constant) are supersingular (case (5) in [5]), and the number of their isomorphism classes does not depend on the behaviour of the isomorphisms at infinity. The remaining case $(1,1,1)$-cubic does not contain curves in a Koblitz model.

With the notation $q=2^m$, the number $(q-1)(2q^2+q-2)$ of isomorphism classes preserving infinity of Type I curves given in [6,8] may be refined, using the data in [5], as shown in Table 4.

Allowing isomorphisms moving ∞, there is a 1:1 map between Type II curves and Type I curves with $h(x)$ having a double root. Hence the number of classes in both cases equals the number $2q(q-1)$ of classes in the case $(1,3)$ of [5]. Note that the larger amount of isomorphisms makes the values in Table 4 change only if $h(x)$ has two different roots in $\mathbb{F}_q$: such number being $\frac{1}{6}q(q-1)(2q-1)$ (see [5]).

References

[1] E. Bach, J. Shallit, Algorithmic Number Theory, vol. 1: Efficient Algorithms, Found. Comput. Ser., MIT Press, Cambridge, MA, 1996.
[2] P. Birkner, Efficient divisor class halving on genus two curves, in: Proceedings of SAC 2006 – The 13th Annual Workshop on Selected Areas in Cryptography, in: Lecture Notes in Comput. Sci., vol. 4356, Springer-Verlag, 2007, pp. 317–326.
[3] J. Canon, W. Bosma, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (3–4) (1997) 235–265.
[4] D. Cantor, Computing in the Jacobian of a hyperelliptic curve, Math. Comp. 48 (1987) 95–101.
[5] G. Cardona, E. Nart, J. Pujolàs, Curves of genus two over fields of even characteristic, Math. Z. 250 (1) (2005) 177–201.
[6] Y. Choie, E. Yeong, Isomorphism classes of hyperelliptic curves of genus 2 over $\mathbb{F}_{2^n}$, Cryptology ePrint Archive 2003/213.
[7] Y. Choie, D. Yun, Isomorphism classes of hyperelliptic curves of genus 2 over $\mathbb{F}_q$, in: Australasian Conference on Information Security and Privacy – ACISP, 2002, in: Lecture Notes in Comput. Sci., vol. 2384, Springer-Verlag, 2002, pp. 190–202.
[8] J. Espinosa García, L. Hernández Encinas, J. Muñoz Masqué, A review on the isomorphism classes of hyperelliptic curves of genus 2 over finite fields admitting a Weierstrass point, Acta Appl. Math. 93 (2006) 299–318.
[9] F. Heß, An algorithm for constructing Weierstraß points, in: D. Kohel, C. Fieker (Eds.), Proceedings of ANTS, in: Lecture Notes in Comput. Sci., vol. 2369, Springer-Verlag, 2002, pp. 357–371.
[10] K. Khuri-Makdisi, Linear algebra algorithms for divisors on an algebraic curve, Math. Comp. 73 (2004) 333–357.
[11] I. Kitamura, M. Katagi, T. Takagi, A complete divisor class halving algorithm for hyperelliptic curve cryptosystems of genus two, in: Lecture Notes in Comput. Sci., vol. 3574, Springer-Verlag, 2005, pp. 146–157.
[12] E.W. Knudsen, Elliptic scalar multiplication using point halving, in: Advances in Cryptology–ASIACRYPT'99, in: Lecture Notes in Comput. Sci., vol. 1716, Springer-Verlag, 1999, pp. 135–149.
[13] T. Lange, Formulae for arithmetic on genus 2 hyperelliptic curves, Appl. Algebra Engrg. Comm. Comput. 15 (5) (2005) 295–328.
[14] T. Lange, M. Stevens, Efficient doubling for genus two curves over binary fields, in: H. Handschuh, M.A. Hasan (Eds.), Selected Areas in Cryptography, 2004, in: Lecture Notes in Comput. Sci., vol. 3357, Springer-Verlag, 2004, pp. 170–181.
[15] J. Miret, R. Moreno, A. Rio, M. Valls, Determining the 2-Sylow subgroup of an elliptic curve over a finite field., Math. Comp. 74 (249) (2005) 411–427.
[16] K.W. Wong, E.C.W. Lee, L.M. Cheng, X. Liao, Fast elliptic scalar multiplication using new double-base chain and point halving, Appl. Math. Comput. 183 (2) (2006) 1000–10007.